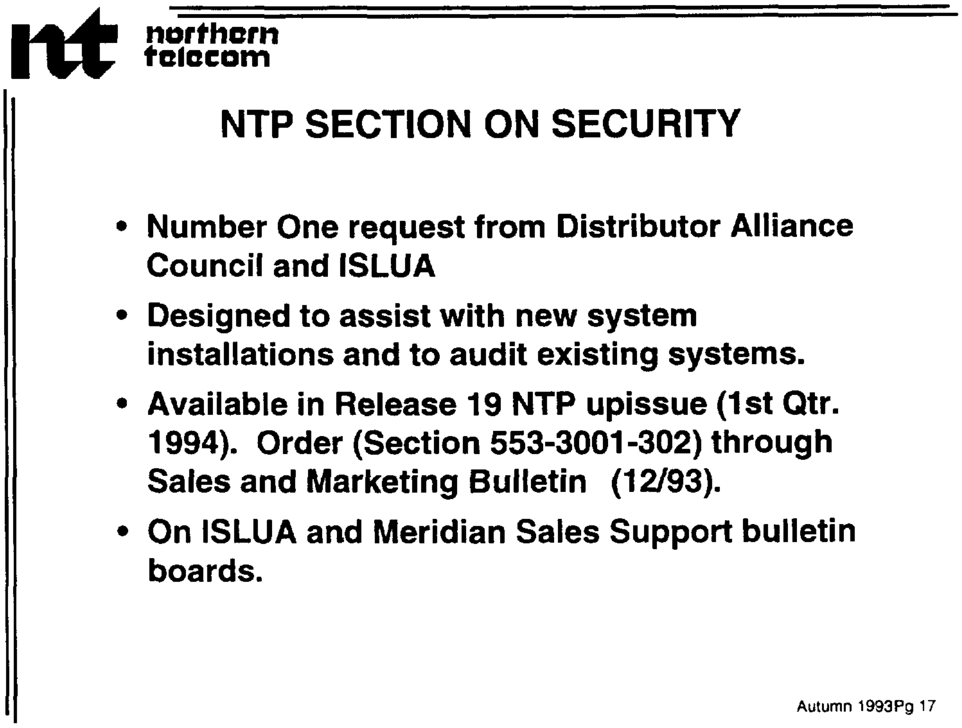


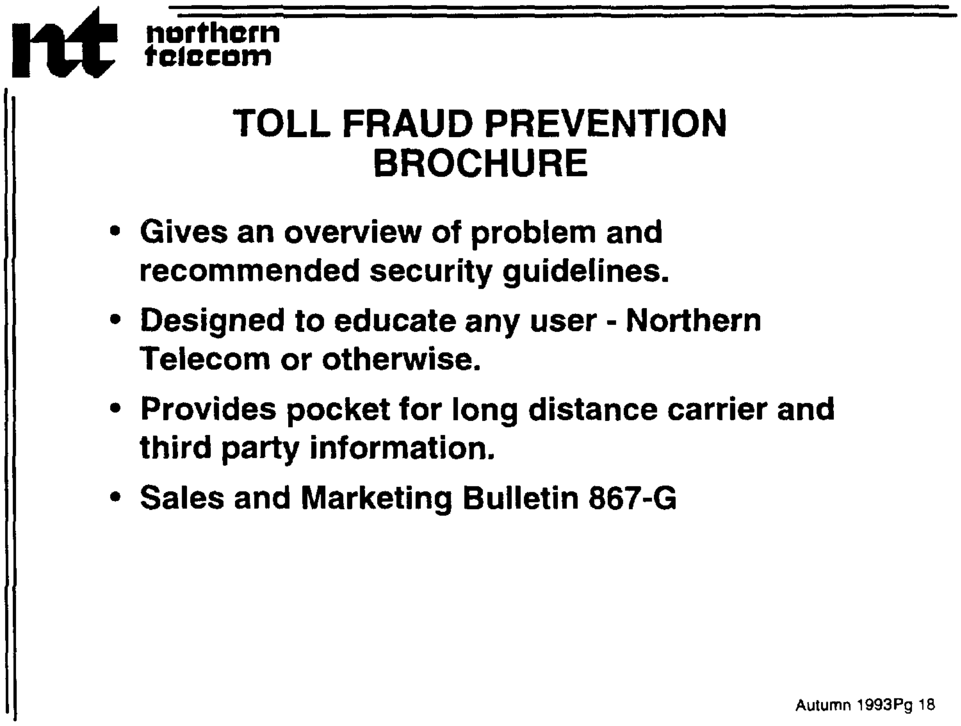
northern telecom

NTP SECTION ON SECURITY

- **Number One request from Distributor Alliance Council and ISLUA**
- **Designed to assist with new system installations and to audit existing systems.**
- **Available in Release 19 NTP upissue (1st Qtr. 1994). Order (Section 553-3001-302) through Sales and Marketing Bulletin (12/93).**
- **On ISLUA and Meridian Sales Support bulletin boards.**

Autumn 1993Pg 17

The number one request received from both the Distributor Alliance Council and the International SL-1 Users Association was the development of an NTP security section. The focus of the section was to instruct users where to find security features in system software and how to activate them. The document becomes available this month through Sales and Marketing and Product Bulletins. It will be included in the Release 19 upissue (1st Qtr. 1994) and can be ordered separately. It will be included in each new shipment beginning in October, instead of the Controlling Access Privileges Workbook currently included in each shipment. The section number is 553-3001-302.

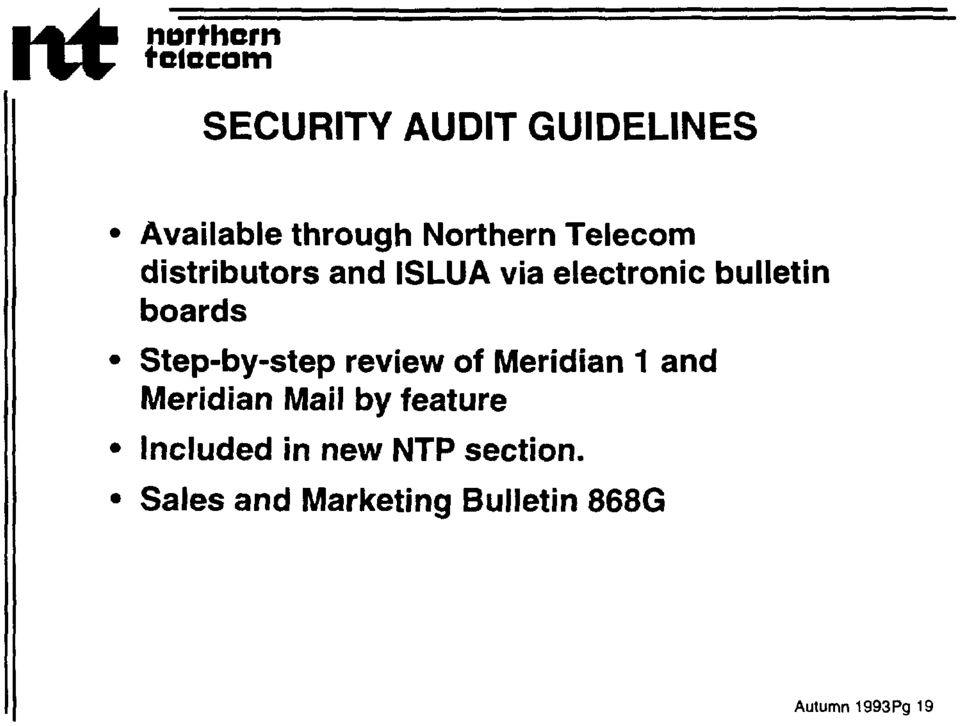


TOLL FRAUD PREVENTION BROCHURE

- Gives an overview of problem and recommended security guidelines.
- Designed to educate any user - Northern Telecom or otherwise.
- Provides pocket for long distance carrier and third party information.
- Sales and Marketing Bulletin 867-G

Autumn 1993Pg 18

Today, you have received our newest toll fraud prevention brochure designed to educate any user about the problem of abuse and fraud. It gives a summary of the problem and security recommendations. It is an excellent document for upper level management, comptrollers, and system users. It also contains a pocket for long distance carrier and third party device information. The brochure is can be ordered in packets of 25. See Sales and Marketing Bulletin 867-G. Speak to your distributor for pricing information.



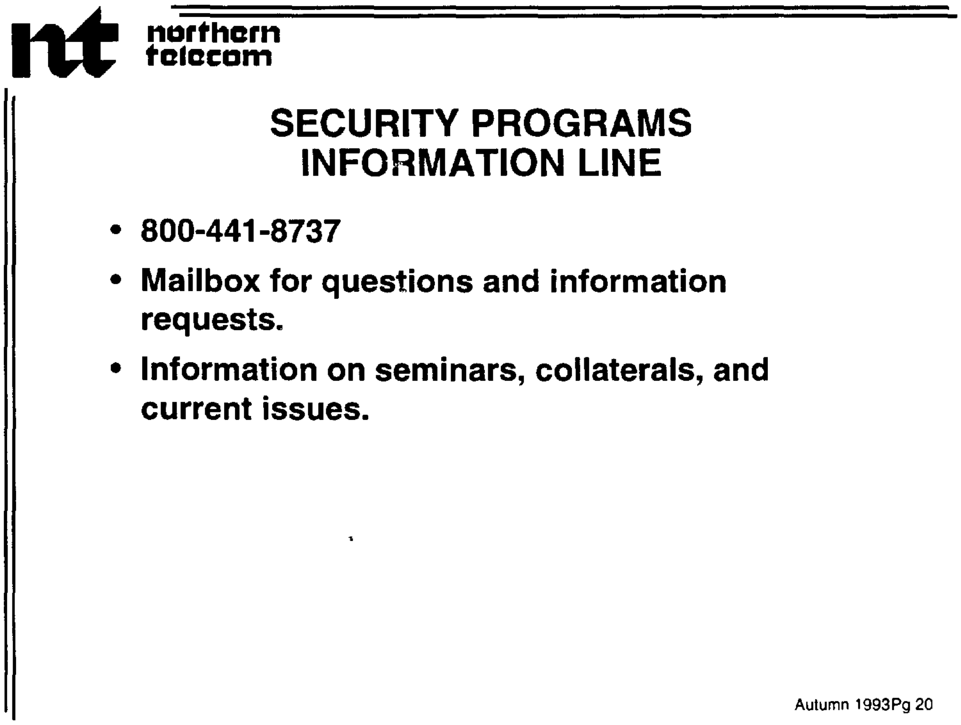
northern telecom

SECURITY AUDIT GUIDELINES

- Available through Northern Telecom distributors and ISLUA via electronic bulletin boards
- Step-by-step review of Meridian 1 and Meridian Mail by feature
- Included in new NTP section.
- Sales and Marketing Bulletin 868G

Autumn 1993Pg 19

In August of 1993, Sales and Marketing Bulletin 868G announced the Security Audit Guidelines for the Meridian 1 and the Meridian Mail. The bulletin is available through Northern Telecom Distributors, the ISLUA bulletin board and the ETAS bulletin board. It presumes a working knowledge of the Meridian 1 system and provides step-by-step review of the Meridian 1 and Meridian Mail. The guidelines are also included in the new NTP section.

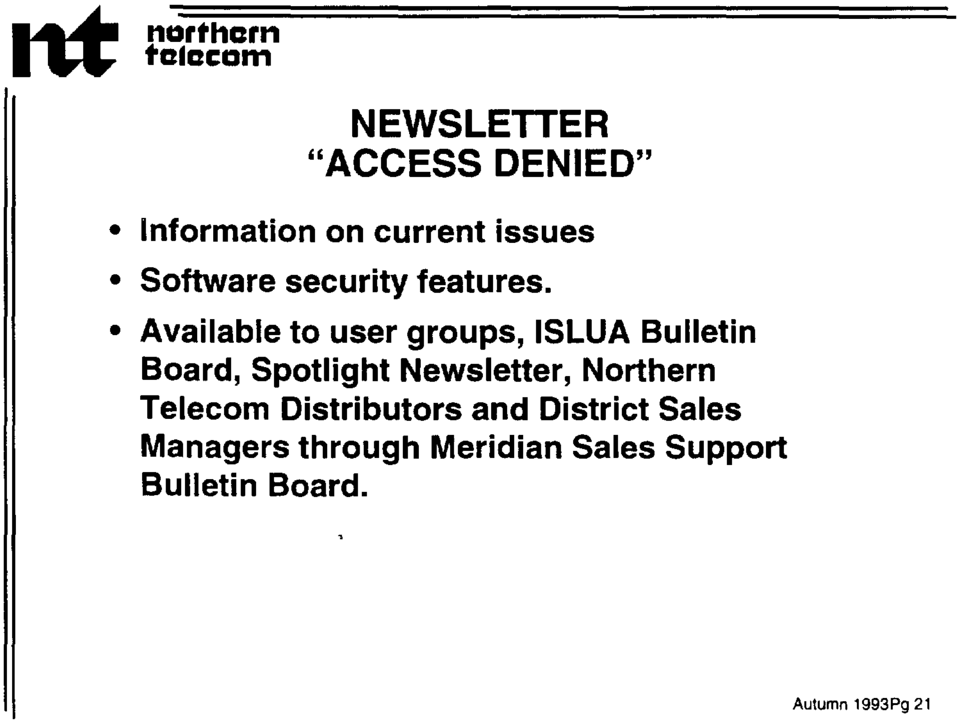


northern
telecom

SECURITY PROGRAMS INFORMATION LINE

- 800-441-8737
- Mailbox for questions and information requests.
- Information on seminars, collaterals, and current issues.

800-441-8737 is the number for the Security Programs Information Line. The menu includes collateral ordering information, a mailbox for questions and information requests, as well as menu selections on seminars and current issues.



northern telecom

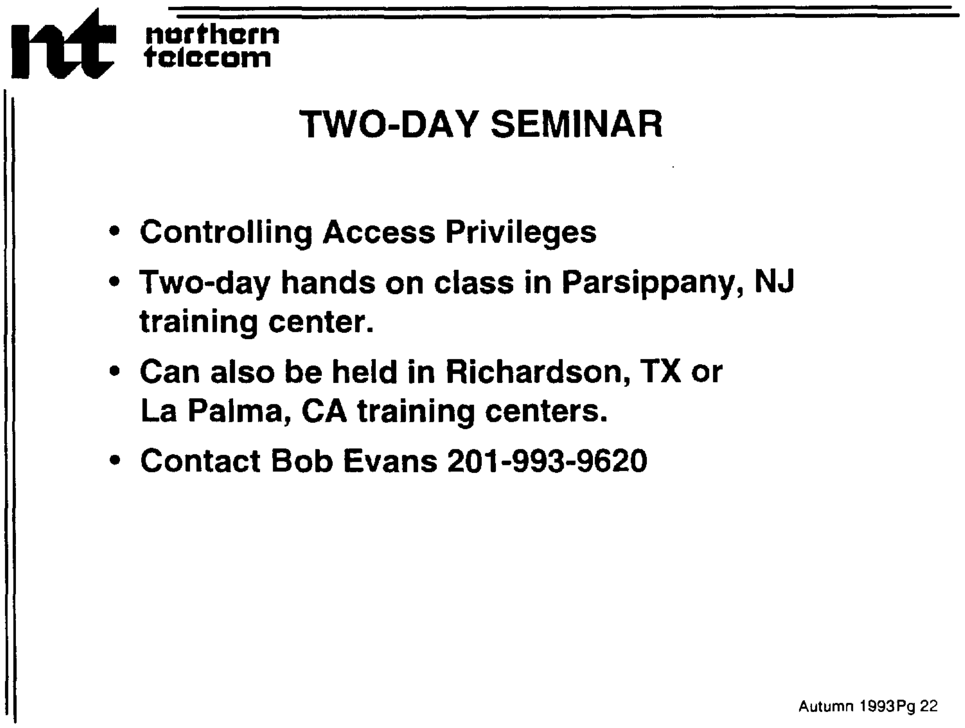
NEWSLETTER "ACCESS DENIED"

- **Information on current issues**
- **Software security features.**
- **Available to user groups, ISLUA Bulletin Board, Spotlight Newsletter, Northern Telecom Distributors and District Sales Managers through Meridian Sales Support Bulletin Board.**

Autumn 1993Pg 21

The newsletter is published quarterly and provides information on current issues such as NXXs in the Dominican Republic, the new "976" equivalent exchanges that are opened when "976" is exhausted in an area code, new features and enhancements that increase security, and new "scams" perpetrated by hackers and how to combat them.

The newsletter is available to user groups, the ISLUA, Northern Telecom Distributors and District Sales Managers through electronic bulletin boards.



northern telecom

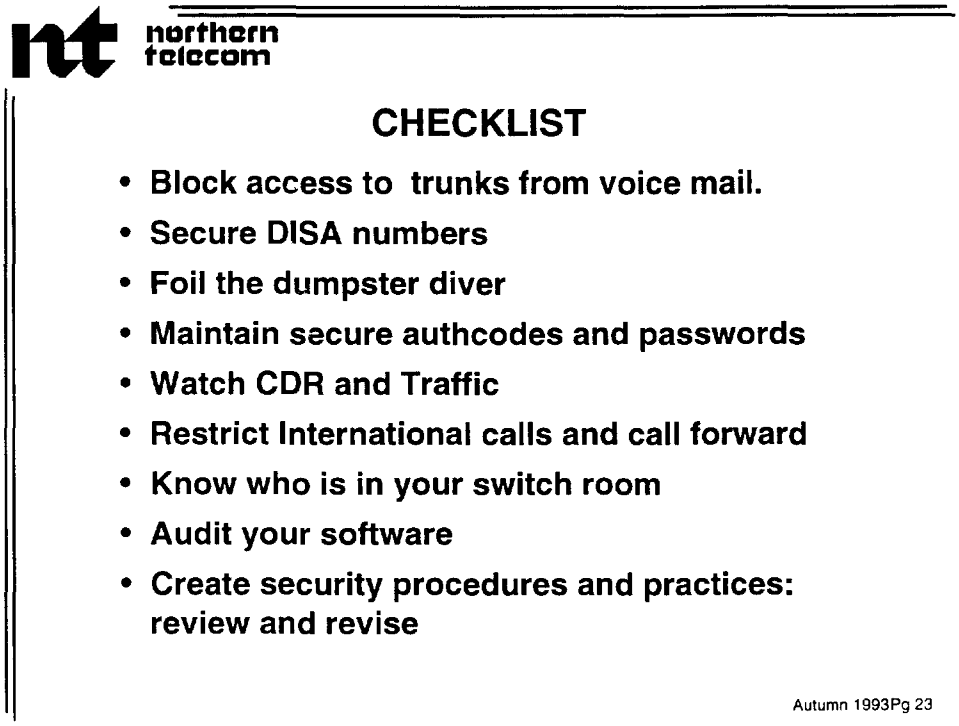
TWO-DAY SEMINAR

- Controlling Access Privileges
- Two-day hands on class in Parsippany, NJ training center.
- Can also be held in Richardson, TX or La Palma, CA training centers.
- Contact Bob Evans 201-993-9620

Autumn 1993Pg 22

Northern Telecom offers a two-day seminar based on the Controlling Access Privileges Workbook. The seminar is two-days of hands on training with the Meridian 1 and Meridian Mail. The seminar is held in Parsippany, NJ, but can also be held in the training centers in Richardson, TX or La Palma, CA.

For more information regarding the seminar schedule, please contact Bob Evans, Manager of the Parsippany Training Center at 201-993-9620.



northern telecom

CHECKLIST

- Block access to trunks from voice mail.
- Secure DISA numbers
- Foil the dumpster diver
- Maintain secure authcodes and passwords
- Watch CDR and Traffic
- Restrict International calls and call forward
- Know who is in your switch room
- Audit your software
- Create security procedures and practices: review and revise

Autumn 1993Pg 23

Check your permission restriction tables to ensure that calls cannot transfer from the voice mail into the PBX. Make sure DISA information is not published in directories or posted. Shred technical and proprietary information. Don't post authcodes. Change them on a regular basis and don't share them. Monitor any system reports that can alert you to unauthorized access. Limit calling capabilities, and restrict call forward. Control access to your switch room and closets. Understand your software. Set up security procedures; review and revise practices when your corporate policies and ways of doing business change.

MCS Multimedia Communication Systems

Sales and Marketing Bulletin

Number: 868-G

Date: August 1993

Meridian Mail Voice Processing Security Audit Guidelines

Toll fraud is a major concern for the telecommunications industry worldwide. Frequently, administrators and distributors request guidelines for providing prompt and response lists that highlight security features.

As an adjunct to the *Controlling Access Privileges* workbook shipped with each new system and upgrade, the *Meridian Mail Voice Processing Security Audit Guidelines* identifies specific areas for review and evaluation. Based on the system's corporate culture and software packages, it is not always possible to invoke every available security feature. These guidelines highlight areas of protection and how to invoke them to provide the most security for a Meridian 1 PBX and Meridian Mail.

The attached list indicates the printouts required for an audit based on the system software configuration. It instructs users on which prompts to review and what the system responses indicate. The guidelines also explain the feature capabilities users can implement or activate as required to provide adequate system security.

Security is almost always a trade-off for convenience. Internal structure must be considered when implementing new or enhanced features. Northern Telecom (NT) recommends implementing the most security options possible to protect the system from unauthorized toll access.

Meridian 1 X11 Release 16 (Limited Access to Overlays) is the minimum recommended software release that provides maximum security options for the Meridian 1 system. Limited Access to Overlays provides increased security with the enhancement of alphanumeric passwords up to 16 characters in length, up to 100 user-definable passwords that restrict access to certain software programs, and the introduction of an audit trail with lockout features. The system tallies invalid log-ons against a predefined threshold, and when the threshold is reached, it disables the port being used. In addition, the system sends messages to other maintenance ports that indicate that an invalid log-on threshold was exceeded. The next terminal to log on receives a message indicating the lockout. The audit trail shows which passwords the previous user entered to access the system and which programs the user accessed when. Security features allow users to define the number of invalid attempts allowed, the amount of time the port is locked out, and whether or not manual system initialization can override the lockout.

Meridian Mail Release 7.54CD is the minimum NT recommends. Refer to Sales and Marketing Bulletin 828-G (Product Bulletin 93003) for additional information on Release 7.54CD. Contact your authorized Meridian 1 distributor for upgrade package information, which indicates the current security features.

How to Use the Guidelines

The auditor should be familiar with Meridian 1 and Meridian Mail software and able to recommend changes associated with database reconfiguration for increased security.

Use the security audit guidelines as follows:

1. Print the appropriate Meridian 1 and Meridian Mail databases based on the attached list.
2. Label each printout for future reference.
3. Compare the prompts and responses appearing on the printouts to the description of the security prompts and responses for each program.
4. Highlight any discrepancies and make changes accordingly.

   If changes require customer or corporate approval, note the security feature affected, how to modify it, and the disadvantages of leaving the feature.
5. Based on comparison findings, either modify the system to increase security or prepare a written report to address the results of the audit and any recommendations for increased security.

Refer to the *X11 Software Feature Guide* section of Northern Telecom Publication (NTP) 553-3001-305 for further clarification of a feature.

Meridian 1 Printouts

Print the following to perform a security audit for Meridian 1 and Meridian Mail systems.

- LD 22 for all software

  CFN—Configuration Record

  PWD—Passwords

  DNB—Directory Number Database

- LD 20 for all software

  TNB—TN Base by telephone type

  TNB—TN Base by trunk type

  SCL—Speed Call Lists

- LD 21 for all software

  CDB—Customer Data Blocks

  RDB—Route Data Blocks

  CRB—Code Restriction Blocks

  SDP—Secure Data Password

- In LD 22, print PKG, GEN, TID, and ISS. Based on the PKG contents, print the following:

  - If PKG contains ACDA, ACDB, ACDC, ACDD, or BACD, print:

    LD 23—all ACD DN data blocks

  - If PKG contains DISA, print:

    LD 24—all DISA data blocks

  - If PKG contains NFCR (X11 Release 2 and above), print:

    LD 49—all New Flexible Code Restriction Trees

  - If PKG contains ODAS, print:

    LD 81—TN list of CFXA

    LD 81—TN list of UNR

  - If PKG contains ESN, BARS, NARS, or CDP, print:

    LD 86—ESN data block

    LD 86—Route List Indexes

    LD 86—Digit Manipulation Tables

- If PKG contains CDP, print:

  LD 87—CDP data blocks DSC, LSC, and TSC

- If PKG contains ESN, CDP, BARS, NARS, or NFCR, print:

  LD 87—Network Control (NCTL)

  LD 87—Free Calling Area Screening (FCAS) tables

- If PKG contains NAUT or BAUT, print:

  LD 88—AUB and AUT

- If PKG contains BARS, NARS, or CDP, print:

  LD 90—AC1 and AC2

  LD 90—NPA

  LD 90—NXX

  LD 90—SPN

  LD 90—LOC

- If PKG contains TENS (multitenant), print:

  LD 93—TENS, CPG, TACC, RACC, TCPG, and RCPG

- If ISS is X11.15 or above, print:

  LD 97—SYSP

Meridian Mail Printouts

Releases 5 and 6

Print the Voice Security Option screen, including through-dialing restrictions, invalid log-in attempt threshold, minimum password length, forced password change, number of entries before repeat password, and expiration warning message parameters.

Release 7

Print the Voice Security Options screen, including invalid log-in attempt threshold, minimum password length, forced password change, number of entries before repeat password, expiration warning message parameters, permission restriction tables for mailboxes, out calling, and custom revert. Also print the Voice Menu restriction table.

Release 8 and Above

Print the Voice Security Options screen, including invalid log-in attempt threshold, minimum password length, forced password change, number of entries before repeat password, expiration warning message parameters, permission restriction tables for mailboxes, out calling, and custom revert. Also print the voice menus to review the permission restriction tables associated with each voice menu.

Releases 5 and 7

Print the Voice Services DN table from the Voice System Administration screen to identify all accesses to voice mail.

Audit Guidelines

These guidelines assume an in-depth working knowledge of the Meridian 1 PBX software, including prompts and responses. Contact your NT distributor for assistance with conducting this audit if you are not trained and certified in Meridian X11 software and/or Meridian Mail software.

Configuration Record—LD 22

Passwords. Identify the following information for all passwords:

LAPW	________________
PWnn	________________
OVLA	________________
CUST	________________
TEN	________________
HOST	Yes or No
OPT	CFPD (A or D)
	LLCA (A or D)
	PRDA (A or D)
	PSCD (A or D)
LPWD	________________
FLTH	________________
LOCK	________________

1. Verify all passwords.
2. Ensure that all passwords have been changed from the default value.
3. Make all passwords complex, alphanumeric, nonrepetitive entries.
4. Change all passwords that are obvious; for example, 123456, 654321, 111222333, the company name, user names, spouses' or children's names, social security numbers, birth dates, employee IDs, or telephone numbers. If the system is from Meridian X11 Release 3 to Meridian 1 X11 Release 15, passwords can be a combination of alphanumeric characters 0 through 9 and A through F. Use this capability to increase password complexity in lower issue machines.

Limit access to overlays by assigning specific passwords. Not all users need access to all software overlays. Where necessary, ensure that users can change their own passwords.

Audit File (Release 16 and above). Define the following Audit Trail statistics:

AUDT Yes or No

SIZE ________________

INIT Yes or No

1. Determine if an Audit File exists.
2. If there is no file, activate one.
3. Ensure that the file is large enough to hold all possible entries.
4. Increase the size if necessary.

Refer to the LD 17 System and Limited Access Password section of NTP 553-3001-400 for information on how to program the software. INIT = YES indicates that manual initialization can reset a port locked out because of invalid log-on attempts.

History File. Define the following History File statistics:

HIST ________________

ADAN ________________

USER ________________

1. Verify that a History File exists.
2. Ensure that the file is large enough to hold the activity directed to it.
3. Review the type of messages being sent to the history file.
4. Print the history file to verify.
5. Eliminate all unnecessary messages.

Call Detail Recording. Identify the following information for this Serial Data Interface (SDI) port:

ADAN TTY______________

USER CTY or CDR

CLID Yes or No

1. Identify which port is assigned Call Detail Recording (CDR) output.
2. Start to ensure activity.

If there is no CDR, disregard all other references to CDR in this document.

Background Terminal. Identify the following information for this SDI port:

ADAN TTY____________

USER BGD

CUST _______________

Identify if a BKG terminal exists and is used to control the class of service.

Traffic Terminal. Identify the following information for this SDI port:

ADAN TTY____________

USER TRF

CUST _______________

1. Identify the traffic terminal.
2. Determine from LD 2 when traffic programs are scheduled.
3. Verify which reports are scheduled and how often they are checked.
4. If there is a third-party device that captures and processes traffic information, identify the hardware and software.

Customer Data Block—LD 21

Night Numbers. Verify the following for each customer:

NITE _______________

NIT1 _______________

TIM1 _______________

NIT2 _______________

TIM2 _______________

NIT3 _______________

TIM3 _______________

NIT4 _______________

TIM4 _______________

1. Identify the night numbers and determine if any NITE data networks (DNs) are Meridian Mail Automatic Call Distribution (ACD) DNs.

2. Indicate those that are Meridian Mail ACD DNs (denoted by an M after the number).

3. Note when the NITE DNs are in use.

Call Forwarding: Forwarding or Originating Control. Verify the following for each customer:

OPT = CFF or CFO

If CFO, CLS, TGAR, and NCOS on DID trunks = ____________

Note: The OPT = CFF or CFO prompt affects only Direct Inward Dialing (DID) calls. The CFO option indicates that the originator of the call has the controlling class of service when the called telephone is in call-forward-all-calls mode. If OPT = CFO, check the Class of Service (CLS), Trunk Group Access Restriction (TGAR), and Network Class of Service (NCOS) of the DID trunk and route data blocks. Restrict DID trunks from external calling, long-distance capabilities, and direct access by other trunk groups. The CFF option indicates that the station being called carries the controlling class of service for call processing in call forward all calls.

Call Detail Recording. Verify the following for each customer:

CDR port assigned ____________

CDPR Yes or No

1. Ensure that the teletypewriter (TTY) port assignment for the CDR matches the port assignment in the Configuration record.
2. If the system is equipped with Coordinated Dialing Plan (CDP), verify whether Coordinated Dialing Plan Record (CDPR) is yes or no.
3. If the answer is yes, a special format is used for CDP calls.

Check the Special Features Guide for more information (NTP 553-2631-100).

Secure Data Password. Verify the following for each customer:

SWPD ____________

Verify that a password exists to change authorization codes and Direct Inward System Access (DISA) information. If the default password is still in place and DISA and AUTH codes are used, change the password to protect the system.

Forced Charge Account. Verify the following for each customer:

CHLN ____________

FCAF Yes or No

CHMN ____________

FCNC ____________

If FCAF = Yes, identify the number of digits in the forced charge account, the minimum number of digits, and the network NCOS for the network forced charge account.

Call Forward to Trunk Access Codes (Release 12 and Above). Verify the following for each customer:

CFTA Yes or No

This prompt should be set at No. If you allow forwarding to trunk access codes, users can forward incoming calls to outbound trunks. If a telephone is TGARed out of direct access, this feature is not active even if allowed.

Controlled Class of Service. Verify the following for each customer:

CCRS (Release 7 and above) ________________

ECC1 (Release 15 and above) ________________

ECC2 (Release 15 and above) ________________

Identify the three (maximum) class of service assignments.

Station Control Password Length. Verify the following for each customer:

SCPL ________________

Indicate the number of digits allowed for a station control password. The recommended minimum is six.

New Flexible Code Restriction. Verify the following for each customer:

NFCR Yes or No

MAXT ________________

Route Data Block—LD 16

Provide the following information for each route:

ROUT ________________

TKTP ________________

PRIV ________________

ISDN ________________

AUTO Yes or No

ICOG ________________

ACOD ________________

TARG ________________

CPDC Yes or No

CDR Yes or No

- INC Yes or No
- QREC Yes or No
- OAL Yes or No
- OTL Yes or No
- AIA Yes or No
- OAN Yes or No
- OPD Yes or No
- NATL Yes or No
- TDG ________________

FRL ________________

1. Using the TGAR worksheet, fill in the access code, trunk type, and TARG for each route as a horizontal entry.
2. For trunks where TYPE = TIE, ISDN = YES, and ISAR = YES, record the following:

   NCOS ________________

   CLS ________________

   TGAR ________________
3. Highlight all AUTO routes and label any routes that are DISA or autoterminating to the automated attendant.
4. Verify that all routes programmed as ICT or OGT are sent one way from the central office. The caution here is that some trunks are two-way from the central office and programmed as one-way at the PBX, inadvertently allowing access to or from the public network.

   Routes programmed as CPDC = Yes are unable to be transferred to another route for outbound traffic. This is a systemwide parameter and effective for any calls using the route. There is no override.
5. Ensure that all routes carrying outbound traffic are programmed to output CDR and identify the types of CDR they are programmed to output.
6. If the route uses with New Flexible Code Restriction (NFCR), note the Facility Restriction Level (FRL) and tree number.

System Speed Call—LD 18

Identify the following:

LNSO ________________

NCOS ________________

STOR ________________

Verify lists and entries.

ACD Data Block—LD 23

List the following information for each ACD DN:

ACDN ____________________

Voice Mail DN Yes or No

NCFW ____________________

Virtual Agent Position IDs and Associated TNs

____________________ ____________________

____________________ ____________________

____________________ ____________________

____________________ ____________________

____________________ ____________________

____________________ ____________________

____________________ ____________________

____________________ ____________________

____________________ ____________________

____________________ ____________________

____________________ ____________________

____________________ ____________________

1. Identify the ACD DNs associated with Meridian Mail.
2. Highlight each night number that is a Meridian Mail ACD DN.
3. List the system software for each virtual agent position ID and TN.
4. Review to ensure that each ID and TN is the lowest NCOS, FRL, CLS possible and cannot directly access any outbound trunk route.
5. Flag any exceptions.

DISA

Verify the following information for each DISA DN:

SWPD ____________________

DN ____________________

SCOD ____________________

AUTR Yes or No

TGAR ____________________

NCOS ____________________

COS ____________________

If there are no DISA DNs active on the system, there are no plans to activate DISA, and the DISA software is resident on PKG, consider having DISA removed from the base software (diskettes or tapes). Eliminate the possibility of database abuse whenever possible.

Determine if security and authorization codes are required. Each DISA DN should not be able to access trunks directly by using access codes. DISA DNs requiring authorization codes should carry a low class of service and NCOS. The authorization code is the mechanism that overrides the DISA DN's class of service.

Code Restriction—LD 19

Identify the following:

ROUT ________________

CLR ALOW or DENY

ALOW or DENY ________________

1. Review the ALOW and DENY entries for each Code Restriction Block (CRB) on each route and indicate those that permit long-distance dialing and have no Basic Automatic Route Selection (BARS) or Network Automatic Route Selection (NARS) to control routing.
2. Identify all programming for Feature Group D:

FGNO ________________

CCAN ________________

LDAC AC1 or AC2

LAAC AC1 or AC2

OPER ________________

INIT ________________

If the system is required to permit the Equal Access Capability, verify that only operator-assisted or credit card calls are accessible. Allowing direct dialed equal access capabilities affects all stations, DISA DNs, authorization codes, TIE trunks, and voice mail virtual agent ports.

New Flexible Code Restriction—LD 49

Review the following for all IDC and FCR entries:

DCNO ________________

IDGT ________________

CRNO ________________

ALOW and/or DENY ________________

BYPS ________________

Identify the trees used for Feature Group D, all trees allowing long-distance calls, and operator-assisted calls.

If the system is required to permit the Equal Access capability, verify that only operator-assisted or credit card calls are accessible. Allowing direct-dialed equal access capabilities affects all stations, DISA DNs, authorization codes, TIE trunks, and voice mail virtual agent ports.

Trunks—LD 14

Verify the following information for each trunk if applicable:

NCOS ______________

NITE ______________

ATDN ______________

TGAR ______________

FCAR Yes or No

CLS ______________

1. Enter the TGAR information on the TGAR matrix for trunks, DISA DNs, authorization codes, and stations.
2. Determine if night DNs are Meridian Mail ACD DNs.
3. Ensure that NCOS, TGAR, and CLS are restrictive enough to prohibit direct access to other outbound trunks and long-distance calling.

Unless trunks tandem through the system for either a network hop-off application or on-net Electronic Switched Network (ESN) call, the trunks should not have the ability to access other outbound facilities.

Stations—LD 10

Identify the following for each single-line telephone:

TGAR ______________

NCOS ______________

SCPW ______________

CLS ______________

(UNR, CFXA, CCSA, TENA, ICDA)

TEN ______________

FCAR Yes or No

FTR

- CFW (number of digits) ______________
- EHT ______________
- EFD ______________
- SSU ______________

1. Note all virtual ports used for accessing a voice mail system.
2. Ensure that the ports are as restricted as possible to prohibit calls from transferring out of the voice mail system to the PBX and making unauthorized toll calls.

3. Enter the TGAR definitions on the TGAR matrix. The matrix displays the direct access capabilities of single-line telephones. TARGS and TGARS that are the same do not receive direct access. All single-line telephones should be restricted from direct access by outbound facilities unless no BARS or NARS software is programmed to process calls. If direct access is the only method of making outbound calls from single-line telephones, review Code Restriction and New Flexible Code restriction data blocks to ensure authorized access of facilities.

4. Assign Station Control Passwords (SCPWs). They should be as long as possible. Codes with up to eight digits are permissible, and each SCPW should be unique.

5. Verify that Call Forward digits are no greater than necessary. If the system has 4-digit extensions, CFW4 is sufficient.

   All telephones should be programmed as CFXD class of service. This prohibits call forwarding to access codes such as AC1, AC2, and numbers external to the PBX. There should be very rare exceptions of external call forwarding.

Note: Unrestricted class of service is just that—unrestricted. Conditionally Toll Denied (CTD) is recommended. Use TLD, SRE, FRE, FR1, and FR2 whenever possible.

6. Identify all telephones that hunt or forward no answer out of the system and their hunt or no answer location. (Restrict this ability whenever possible.)

7. Indicate stations that are assigned CCSA, SSU, FCA, and/or TENA. When active, these features indicate possible access restrictions and controls.

Stations—LD 11

Identify the following for each multiline telephone:

TGAR ________________

NCOS ________________

SSU ________________

SCPW ________________

CLS ________________

(UNR, CFXA, CCSA, TENA, ICDA)

EFD ________________

EHT ________________

TEN ________________

FCAR Yes or No

KEY

- CFW (number of digits) ________________
- CHG ________________

1. Note all virtual ports used for access to a voice mail system.

2. Ensure that the ports are as restricted as possible to prohibit calls from transferring out of the voice mail system to the PBX and to prevent unauthorized toll calls.

3. Enter the TGAR definitions on the TGAR matrix. The matrix displays the direct access capabilities of multiline telephones. All multiline telephones should be restricted from direct access by outbound facilities unless no BARS or NARS software is programmed to process calls. If direct access is the only method of making outbound calls from multiline telephones, review Code Restriction and New Flexible Code Restriction data blocks to ensure authorized access by facilities.
4. Assign SCPWs. They should be as long as possible. Codes up to eight digits are permissible, and each SCPW should be unique.
5. Verify that Call Forward digits are no greater than necessary. If the system has 4-digit extensions, CFW4 is sufficient.

   All telephones should be programmed as CFXD level of service. This prohibits call forwarding to access codes such as AC1 and AC2 and numbers external to the PBX. There should be very rare exceptions of external call forwarding.

Note: Unrestricted class of service is just that—unrestricted. Conditionally Toll Denied (CTD) is recommended. Use TLD, SRE, FRE, FR1, and FR2 whenever possible.

6. Indicate stations that are assigned CCSA, SSU, FCA, and/or TENA. When active, these features affect access restrictions and controls.

Flexible Feature Codes—LD 57

Identify the following feature codes:

ASRC ________________

AUTH ________________

CDRC ________________

CFWA ________________

CFWD ________________

CFWV ________________

DEAF ________________

ELKA ________________

ELKD ________________

RCFA ________________

RCFD ________________

RCFV ________________

SCPC ________________

SSPU ________________

These features activate access features such as Call Forward (internally and remotely) Electronic Lock, System Speed Call (SSC), and SCPW change.

Electronic Switched Network—LD 86

ESN Data Block. Identify the following for each ESN data block:

CDP Yes or No

- MXSC ____________
- NCDP ____________

AC1 ____________

AC2 ____________

TODS ____________

____

____

____

____

____

____

RCTL Yes or No

- NMAP ____________
- ETOD ____________

TGAR Yes or No

1. Verify if the system uses the Coordinated Dialing Plan feature and how many digits are in a steering code.
2. List codes for AC1 and AC2
3. List time schedules for TODS.
4. Indicate if Restricted Control (RCTL) is used and when it is effective.
5. State if TGAR is used in addition to the standard BARS or NARS controls to access trunk routes.

   TGAR control is commonly used in multi-tenant environments.

Digit Manipulation Index. Identify the following for each Digit Manipulation Index (DGT):

DMI ____________

DEL ____________

INST ____________

1. Note any DGTs that delete internal numbers and insert complete external numbers.
2. Verify that these numbers are valid, especially if they are routed to another area code.

Route List Index. Identify the following for each Route List Index (RLI).

RLI ______________

ENTR ______________

ROUT ______________

TOD ______________

CNV Yes or No

EXP Yes or No

FRL ______________

DMI ______________

FCI ______________

MFRL ______________

1. Note any RLIs that deviate from consistent programming, such as no TODs, DGTs to external numbers, low FRLs, no FCAS tables for long-distance routing, or unusual route patterns.
2. Note which Numbering Plan Area Codes, Central Office Translations, Special Number Translations, Distant Steering Codes, Trunk Steering Codes, or Location Codes are routed to these RLIs.

Incoming Trunk Group Exclusion Index. Identify the following for each Incoming Trunk Group Exclusion Index (ITGE):

ITEI ______________

RTNO ______________

1. Determine which numbers ITGEs are blocking.
2. Determine if the ITGEs are programmed effectively .
3. Test to ensure correct application.

Electronic Switched Network—LD 87

Coordinated Dialing Plan (CDP). Identify the following for each Distant Steering Code (DSC), Local Steering Code (LSC), and Trunk Steering Code (TSC).

LSC, DSC, or TSC ______________

DEL (LSC) ______________

RLI (DSC, TSC) ______________

Network Control. Identify the following for the Network Control (NCTL):

NCOS ______________

- FRL ______________
- RWTA Yes or No
- NSC Yes or No
- LIST Yes or No